Attorney Docket # 526801-57RCE Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Jorge SEVILLA ABELLAN et al. Serial No.: 10/561,012 Filed: December 11, 2006 For: Databases Synchronization	Examiner: MAHMOOD, Rezwanul Group Art: 2164

Mail Stop **AF**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRE-APPEAL BRIEF REQUEST FOR REVIEW

SIR:

This is a Request for a Panel Review of Issues on Appeal. A Notice of Appeal is filed concurrently herewith in response to the final Office Action dated February 11, 2011. No amendments are being filed with this Request.

Arguments supporting the Request for Review begin on page 2 of this Request.

ARGUMENTS

The matters to be reviewed are whether claims 2-4, 6, 7, 10 and 11 are unpatentable under 35 USC § 103(a) as obvious from U.S. Patent 6,505,215 ("Kruglikov") in view of U.S. Patent 6,813,498 ("Durga"), U.S. Patent 6,824,064 ("Guthery"), and further in view of U.S. Patent 6,779,002 ("Mwaura"), and whether claim 8 is unpatentable under 35 USC § 103(a) as obvious from Kruglikov in view of Durga, Guthery, Mwaura, and U.S. Patent 6,676,022 ("Guthery '022").

Applicants' disclosed embodiments are directed to the synchronization of a database contained in a mobile first data processing system with another database contained in a network operator server (i.e. the "second data processing system"). In accordance with the invention, an operator or network-supplied application is loaded into a security token, such as a SIM card, that is coupled to the mobile first data processing system. The application is operable to request that the mobile first data processing system start a synchronization process between the database stored in the mobile first data processing system and the database stored in the network operator server in accordance with a specific operator/network synchronization policy.

The security token does not contain the database, i.e., the application and the database are separate and located in different devices. In other words, the application loaded in the security token provides a remote command to the mobile first data processing system to start the synchronization process. The security token is thus a third party to the system of the mobile first data processing system and the network operator server. A user of the mobile first data processing system cannot start or initiate synchronization for any database in the mobile first data processing system because such control is located remotely, in the application in the security token, from the mobile first data processing system (which contains the database). Synchronization is instead started automatically by the security token, which does not contain the database. However, it is by operation of the application that the messages or events that occur in the mobile first data processing system or in the network are received, and they are concluded by the application, in response to the messages or events received and in accordance with the synchronization policy, whether a synchronization of the first and second databases is needed.

Kruglikov discloses a system for synchronizing a portable system (110), e.g., a handheld device, with a personal computer (150). The Examiner concedes that Kruglikov does not disclose

"the application configured to remotely request that a mobile data processing system start a process and receiving a remote command." (See the Final Office Action at page 3). The Examiner instead asserts that Durga discloses a programming stored in a mobile unit configured to remotely start a process and receiving remote instructions.

Durga teaches that when a mobile unit has been reported to be missing, such as lost or stolen, an adjunct network entity, such as an intelligent network server, which has a detection and recovery application, determines or assigns a recovery identification and a recovery channel for the missing mobile unit. The mobile switching center then transmits a distinctive recovery page to the mobile unit via the base station, in which the recovery page includes information specifying the recovery identification and the recovery channel. The mobile unit, upon reception of the recovery page, enters a recovery mode and transmits a recovery signal on the recovery channel, with the recovery signal including the recovery identification. (See col. 1, line 63 through col. 2, line 11 of Durga).

But the programming stored in Durga's mobile unit is not configured to remotely request that the mobile unit start a synchronization process of the mobile unit with the mobile switching center. Indeed, the Examiner acknowledges that the programming is stored in the mobile unit. Moreover, the mobile unit enters the recovery mode and transmits the recovery signal on the recovery channel upon reception of a recovery page. Accordingly, the request to start the recovery process does not even come from the programming stored in the mobile unit in Durga; it comes instead from the completely separate and different detection and recovery application which is stored in the adjunct network entity via the mobile switching center. That is, it comes from a completely separate data processing system, other than the mobile unit, that is not coupled to the mobile unit. Nowhere does Durga identify or delineate an application configured to remotely request that the mobile unit start a synchronization process, wherein it is by the application that the messages or events that occur in the mobile unit or in the network are received, and it is concluded by the application, in response to the messages or events received and in accordance with the synchronization policy, whether a synchronization of the first and second databases is needed.

Furthermore, the Examiner (at page 4 of the Final Office Action) acknowledges that Kruglikov and Durga do not explicitly disclose a security token coupled to the mobile first data

processing device, and loading the application in the security token. The Examiner further cites Guthery as purportedly teaching "a security token coupled for communication with the mobile first data processing system and an application being loaded into the security token."

Guthery relates to a smart card capable of storing a number of applications and a memory that is logically partitioned into a number of memory blocks. Guthery's system seeks to allow simultaneous communication with more than one of the applications. To do so, it is necessary to dynamically allocate the scarce memory of the smartcard. This is done using a control program stored on the smartcard. (See Abstract of Guthery and col. 2, lines 52-58).

Guthery does not address database synchronization and, therefore, does not teach or suggest "loading an application into a security token coupled to the mobile first data processing system, the application configured to remotely request that the mobile first data processing system start a synchronization process of the first database with the second database according to a synchronization policy" and "if a synchronization is needed, transmitting, by the application, a remote command to the mobile first data processing system that informs the mobile first data processing system that a new synchronization is requested, said remote command providing the mobile first data processing system with information about synchronization parameters for use in synchronizing content of the first and second databases", as expressly recited in Applicants' independent claim 10. Guthery, therefore, does not remedy the deficiencies of Kruglikov and Durga, discussed above, with respect to these claimed features.

Moreover, the Examiner contends that Guthery broadly teaches "loading the application in the security token." However, Guthery does not teach that any application can or should be loaded into the smartcard, as the Examiner suggests. Rather, Guthery simply teaches the use of multiple conventional security-related applications on a smart card, such as for use with credit card terminals, automated teller machines (ATMs), and mobile phones, with the additional inclusion on the smart card of a memory administration program that allows simultaneous communication with these various on-card applications while dynamically allocating the smartcard's scarce memory:

> The present invention provides tight linkage between the communication with smart card applications, allocation of scarce resources within the smart card, and the scheduling of execution of those applications. The system and method is constructed to embrace and be compatible with current modes of smart card usage.

(Guthery at col. 7, lines 36-42).

Therefore, even assuming, *arguendo*, that Kruglikov and Durga disclose the claimed application "configured to remotely request that the mobile first data processing system start a synchronization process of the first database with the second database according to a synchronization policy," as the Examiner contends (which Applicants have expressly refuted above), the combination of Kruglikov, Durga and Guthery would not teach or suggest a first database that is stored in a portable system remote from a synchronization program loaded into the smartcard, or that a remote command is provided to the portable system from the smart card to start the synchronization process. Rather, this combination of references would, at most, teach the use of a smartcard as a security device, with the synchronization program being stored on the portable system, rather than in the smartcard, because that is where Kruglikov and Durga expressly teach that the synchronization program and recovery mode programming are stored, and Guthery fails to provide any teaching with respect to such a synchronization program.

Moreover, Guthery describes a plurality of applications that are run at the same time. In contrast, Applicants' claimed invention is directed to only a single application that transmits "a remote command to the mobile first data processing system that informs the mobile first data processing system that a new synchronization is requested". It is only after this synchronization that the mobile first data processing system, which stores the first database remotely from the application, initiates "the synchronization process of the first and second databases in response to receiving the remote command".

The third cited reference, Mwaura, discloses a computer software framework and method for synchronizing data across multiple databases involving the exchange of data synchronization messages. The Examiner cites Mwaura as purportedly teaching receiving a message by an application and determining if synchronization is needed by checking whether the message is relevant and, if so, taking a synchronization action. However, nothing has been found in Mwaura that would remedy the deficiencies of the combination of Kruglikov and Guthery with respect to the features of independent claim 10 discussed above.

Therefore, the Examiner's *prima facie* case in support of the rejection of independent claims 10 suffers from the additional deficiency that the cited references do not disclose the claimed feature: "a first database that is stored in a mobile first data processing system" and

"loading an application into a security token coupled to the mobile first data processing system, the application configured to remotely request that the mobile first data processing system start a synchronization process of the first database with the second database according to a synchronization policy".

Independent claim 10 is accordingly deemed to be patentably distinct over the cited art for at least the foregoing reasons.

It is therefore requested that the rejection of independent claim 10 under 35 U.S.C. § 103, and of all of the claims depending from claim 10, be reversed and the rejection withdrawn.

CONCLUSION

In view of the foregoing, Applicant believes that the present application is now in proper condition for allowance. Prompt and favorable action to this effect and early passing of this application to issue are respectfully solicited.

Respectfully submitted,
COHEN PONTANI LIEBERMAN & PAVANE LLP

By /Lance J. Lieberman/
Lance J. Lieberman
Reg. No. 28,437
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: June 10, 2011